Rational Points on Curves

Lectures by: Steffen Müller
Notes by: Ross Paterson

These notes were taken live during lectures at the CMI-HIMR Computational Number Theory summer school held at the University of Bristol in June 2019. In particular, any mistakes are the fault of the transcriber and not of the lecturer. Remarks in red were not written on the board, and were often added later by the transcriber.

Lecture 4: Mordell-Weil Sieve

Today we talk about yet another method for rational points for which, rather than working with complicated p-adic analysis, we will work with information $\bmod p$. Given $X/\mathbb{Q}$ a nice curve with genus $g \geq 2$, let $J = \operatorname{Jac} X$ and let $X \xhookrightarrow{\iota} J/\mathbb{Q}$ be an Abel-Jacobi map. Assume that generators of $J(\mathbb{Q})$ are given. We have a commutative diagram for p a prime of good reduction.

$$\begin{array}{ccc} X(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow & & \downarrow{\scriptstyle \nu_p} \\ \overline{X}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \overline{J}(\mathbb{F}_p) \end{array} \tag{1}$$

$\iota(X(\mathbb{Q})) \subset \nu_p^{-1}\iota_p(\overline{X}(\mathbb{F}_p)) =: V_p$. Let S be some set of good primes, then

Theorem 0.1 (Scharaschkin)**.** *If $\bigcap_{p\in S} V_p = \emptyset$ then $X(\mathbb{Q}) = \emptyset$.*

Is there any hope of this being true? Well there is a heuristic due to Poonen

Heuristic 1 (Poonen)**.** *If $X(\mathbb{Q}) = \emptyset$ then there exists some S finite such that*

$$\bigcap_{p\in S} V_p = \emptyset$$

In fact this is related to the Brauer Manin obstruction, as was shown by Scharaschkin under assumption that Ш is finite.

Remark 0.2. *Can also:*

- *Work mod p^n for $n > 1$,*
- *Use bad primes*

Suppose that $X(\mathbb{Q}) \neq \emptyset$, and we have $X(\mathbb{Q})_{\text{known}} \subset X(\mathbb{Q})$ we want to show equality. Fix $b \in X(\mathbb{Q})_{\text{known}}$ and let $\iota(P) = [P - b]$ be our fixed Abel-Jacobi map. Let $p \in S$ and $\overline{P} \in \overline{X}(\mathbb{F}_p) \backslash X(\mathbb{Q})_{\text{known}}$. If

$$\nu_p^{-1}(\iota_p(\overline{P})) \not\subset \bigcap_{q \in S} V_q$$

then $\overline{P} \notin \overline{X(\mathbb{Q})}$.

Note that, compared to the version of Chabauty we saw yesterday, this can actually detect when the set of rational points is empty which Chabauty (as we saw it) cannot. More generally, Chabauty uses $\rho : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ where $P \mapsto \int_0^P \omega_0$ for ω_0 an annihilating differential, so that $\rho(X(\mathbb{Q})) = 0$. This means that the zeroes of ρ are precisely $X(\mathbb{Q}) \cup Z \subset X(\mathbb{Q}_p)$, and one can show that $Z \cap X(\mathbb{Q}) = \emptyset$ using congruence conditions and Mordell-Weil Sieve. We adapt the commutative diagram (1) to the set of primes S to look at:

$$\begin{array}{ccc} X(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \nu_S \\ \prod_{p \in S} \overline{X}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \prod_{p \in S} \overline{J}(\mathbb{F}_p) \end{array} \tag{2}$$

Consider $C : Q + NJ(\mathbb{Q})$ for $N \geq 2$ and $Q \in J(\mathbb{Q})$. If $\nu_S(C) \cap \text{im}(\iota_S)$ then there are no rational points on the curve mapping into C, i.e. $\iota(X(\mathbb{Q})) \cap C = \emptyset$. Extending (2) we look now at

$$\begin{array}{ccccc} X(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow \nu_S & & \downarrow \beta_{S,N} \\ \prod_{p \in S} \overline{X}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & \prod_{p \in S} \overline{J}(\mathbb{F}_p) & \longrightarrow & \prod_{p \in S} \overline{J}(\mathbb{F}_p)/N\overline{J}(\mathbb{F}_p) \end{array} \tag{3}$$

we label the composition along the bottom row as $\alpha_{S,N}$. We want $\gcd(N, \#\overline{J}(\mathbb{F}_p))$ to be big for many $p \in S$.

Suppose for some reason you know that $X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})/NJ(\mathbb{Q})$. This gives rise to a method where we try to compute $X(\mathbb{Q})$ as follows:

1. Select suitable S,
2. For all $c \in J(\mathbb{Q})/NJ(\mathbb{Q})$, such that no $P \in X(\mathbb{Q})_{\text{known}}$ maps to c.
   - *By day*, try to show that $\beta_{S,N}(c) \notin \text{im}(\alpha_{S,N})$
   - *By night*, search for rational points $P \in X(\mathbb{Q})$ mapping to C.

Lemma 0.3. *Let $r < g$ and p a good prime, $\omega_0 \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$ an annihilating differential such that $\overline{\omega_0} \in H^0(\overline{X}, \Omega^1) \backslash \{0\}$. Assume that $\overline{\omega_0}(\overline{P}) \neq 0$ for all $\overline{P} \in \overline{X}(\mathbb{F}_p)$. Let $N \geq 2$ be such that N is divisible by the exponent of $\#\overline{J}(\mathbb{F}_p)$. Then*

$$X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})/NJ(\mathbb{Q})$$

is an injection.

Proof. Let $P, Q \in X(\mathbb{Q})$ be such that $\iota(P) - \iota(Q) \in NJ(\mathbb{Q})$. Then $\overline{\iota(P)} = \overline{\iota(Q)}$ since N is divisible by the exponent. But $\overline{\iota}$ is an injection so $\overline{P} = \overline{Q}$. However, $\overline{\omega_0}(\overline{P}) \neq 0$ then $\#D_{\overline{P}} \cap X(\mathbb{Q}) \leq 1$ so $P = Q$. □

We get a practical method to compute $X(\mathbb{Q})$ if $r < g$ and if we can

- Compute $\int_P^Q \omega$ for $\overline{P} \neq \overline{Q}$. There is $n \mid \#\overline{J}(\mathbb{F}_p)$ such that $n[Q-P] = \sum_i [Q_i - P_i]$ where $\overline{Q_i} = \overline{P_i}$ for all i. Then
$$\int_P^Q \omega = \frac{1}{n} \sum_i \int_{P_i}^{Q_i} \omega$$
however $P_i, Q_i \in X(\overline{\mathbb{Q}_p})$, so this may be difficult.
- Use Coleman integration, for which you need a lift of Frobenius to a certain p-adic cohomology group. (See Balakrishnan-Bradshaw-Ketlaya for more details, or Balakrishnan-Tuitman for an extension to greater generality)
- Show $r < g$ (r is rank!) and find r independent points in $J(\mathbb{Q})$ mod $J(\mathbb{Q})_{\text{tors}}$ to find ω_0. We can often work entirely in $\text{Sel}^{(2)}(J/\mathbb{Q})$ (See Poonen-Stoll or Stoll).

Example 1. *This will not use anything we said so far, but do something much simpler.*

$$X : y^2 = x^6 - 4x^4 + 8x^2 - 4$$

Chabauty did not work for this. Consider the quotient elliptic curve obtained via $\varphi : (x, y) \mapsto (x^2, y)$*:*

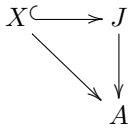
$$E : y^2 = x^3 - 4x^2 + 8x - 4$$

$X(\mathbb{Q}) \subset \varphi^{-1}E(\mathbb{Q})$. *But* $\text{rk}(E(\mathbb{Q})) = 1$*, so no use. However, the Jacobian of* X *is an abelian variety of dimension* 2 *which will contain* E*, so there is another elliptic curve in this. Consider*

$$E' : y^2 = -4x^3 + 8x^2 - 4x + 1$$

obtained by $(x, y) \mapsto (x^{-2}, yx^{-3})$*. Show that* $E'(\mathbb{Q}) = \{\infty, (0, \pm 1), (1, \pm 1)\}$*. Thus* $X(\mathbb{Q}) = \{\infty_\pm, (\pm 1, \pm 1)\}$.

Example 2. *If* $J \sim A \times \dots$ *such that* $\text{rk}(A/\mathbb{Q}) = 0$ *we can use*



If $r = g$ and $\text{rk}(NS(J)) > 1$ (NS here means the Neŕon-Severi group) we can sometimes use non-abelian Chabauty (Kim, Balakrishnan-Dogra,...). Arizona winter school 2020 will be about precisely this, and you are all heartily encouraged to attend.